VULNERABILITY TESTING

ISSP-09-0410

1. **SUBJECT:** In order to assess OPIC's information security posture and determine the security risks that should be mitigated, OPIC will conduct periodic vulnerability assessments. These assessments will assist in the discovery of security vulnerabilities, gauge the threat posed by these vulnerabilities, and assist OPIC with decreasing security risk.
2. **SCOPE:** This policy applies to all OPIC owned or operated systems, networks, applications, data repositories, and other information resources.
3. **DESCRIPTION:** Today's information systems are complex and composed of many interdependent and interconnected components. No matter how well they have been developed, all systems have some inherent vulnerabilities or exploitable flaws. Over time, these vulnerabilities are likely to be exploited, either intentionally or accidentally.

   Security testing is an important means of detecting weaknesses and determining the threat posed by them. It also helps to determine the effectiveness of security measures that have been implemented, and to assess how well the organization can withstand security attacks. A vulnerability testing program provides the crucial details to prepare OPIC to avoid the significant financial costs or damage to its reputation that could result from security malfeasance.

   Because threats, vulnerabilities, and the configurations of the systems themselves are always changing, the Federal Information Security Management Act (FISMA) requires OPIC to perform security testing on a periodic basis. A systematic, comprehensive, ongoing, and priority-driven security testing program will assist OPIC with determining its security priorities and making prudent investments to enhance the security posture of its information resources.

4. **PROCEDURES & GUIDELINES:**

   (a) Vulnerability testing should be conducted at least annually while systems are running in their operational environments.

   (b) Testing should not disrupt critical business operations.

   (c) Procedures for testing should be clearly defined and documented.

   (d) All test results should be well documented.

   (e) If necessary, the "rules of engagement" should be communicated to the system owners.

   (f) Information Owners and Information Custodians should be informed of the results to ensure that vulnerabilities are patched or mitigated.

   (g) All systems should be retested once vulnerabilities are addressed to ensure that they have been effectively mitigated.

(h) Vulnerability testing should be integrated into OPIC's risk management processes.

(i) OPIC will adhere to NIST guidance as set forth in Special Publications 800-42, Guideline on Network Security Testing; 800-51, Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme; 800-53A, Techniques and Procedures for Verifying the Effectiveness of Security Controls in Information Systems, and subsequent publications, as well as other relevant best practices.

5. ROLES & RESPONSIBILITIES:

(a) The Information Systems Security Officer (ISSO) is responsible for:

(1) Developing testing procedures.

(2) Performing periodic testing.

(3) Documenting test results.

(4) Communicating vulnerabilities to Information Owners and Custodians.

(5) Auditing to ensure that vulnerabilities have been mitigated.

(6) Providing advice to Information Owners and Custodians regarding potential mitigation strategies.

(b) Information Owners are responsible for:

(1) Allowing vulnerability testing to be performed on their resources.

(2) Ensuring that any identified vulnerabilities are resolved for their resources.

(c) Information Custodians are responsible for:

(1) Assisting the ISSO with performing security testing, as requested.

(2) Helping Information Owners with selecting and implementing mitigation strategies.

(3) Documenting mitigations that are implemented.

(4) Informing the ISSO about mitigations performed.

6. DEFINITIONS:

(a) Threat - A circumstance, event, or person with the potential to cause harm to a system in the form of destruction, disclosure, data modification, and/or Denial of Service (DoS).

(b) Vulnerability – Any characteristic of a computer system that renders it susceptible to destruction or incapacitation. A design, administrative, or implementation weakness or flaw in hardware, firmware, or software that, if exploited (either intentionally or accidentally), could lead to an unacceptable impact in the form of unauthorized access to information or disruption of critical processing.

(c) Vulnerability Assessment (or Vulnerability Testing) – Systematic examination of a system to determine the adequacy of security measures, identify security

deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

7. **ENFORCEMENT:** Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.
8. **POINT OF CONTACT:** OPIC Information Systems Security Officer (ISSO)
9. **ATTACHMENTS:** None
10. **AUTHORITY:**

(a) OPIC Directive 00-01, Information Systems Security Program.

(b) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002

(c) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.

(d) Homeland Security Presidential Directive / HSPD-7, December 17, 2003

(e) NIST Special Publication 800-42, Guideline on Network Security Testing

(f) NIST Special Publication 800-53A, Techniques and Procedures for Verifying the Effectiveness of Security Controls in Information Systems

(g) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.

11. **LOCATION:** TBD
12. **EFFECTIVE DATE:** October 22, 2004
13. **REVISION HISTORY:** None
14. **REVIEW SCHEDULE:** This policy should be reviewed and updated annually.